REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed June 20, 2005. Upon entry of the amendments in this response, claims 1, 3, 5 – 13, 16 and 18 – 25 remain pending. In particular, Applicant has added claims 21 - 25, has amended claims 1, 3, 6, 12, 13, 16 and 19, and has canceled claims 2, 4, 14, 15 and 17 without prejudice, waiver, or disclaimer. Applicant has canceled claims 2, 4, 14, 15 and 17 merely to reduce the number of disputed issues and to facilitate early allowance and issuance of other claims in the present application. Applicant reserves the right to pursue the subject matter of these canceled claims in a continuing application, if Applicant so chooses, and does not intend to dedicate the canceled subject matter to the public. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

Rejections Under 35 U.S.C. §102

The Office Action indicates that claims 1, 5, 7, 12 and 19 stand rejected under 35 U.S.C. §102(e) as being anticipated by *Klein*. Applicant respectfully traverses the rejection.

In this regard, Applicant respectfully agrees with the contention in the Office Action indicating that *Klein* does not disclose the use of one-time URLs. Additionally, Applicant respectfully asserts that *Klein* does not disclose preventing access to an address after a predetermined period of time has elapsed and/or the encrypted information being provided from a first network device to a second network device without either of the devices being identified to the other. This is in direct contrast to the limitations recited in independent claims 1, 12 and 19 as is described below.

In this regard, claim 1 has been amended to recite:

> 1. A method for securely communicating information, said method comprising:
>
> communicating an address to a first network device via the Internet such that the first network device provides information corresponding to the address for use by a second network device;
>
> receiving encrypted information from the first network device via the Internet;
>
> enabling the encrypted information to be posted at the address; and
>
> enabling the second network device to access the address and retrieve the encrypted information posted at the address;
>
> ***wherein the address provided to the first network device is a first Uniform Resource Locator (URL) configured for a one-time use; and***
>
> ***wherein the second network device retrieves the encrypted information using a second URL, the second URL being configured for a one-time use.***

(Emphasis added).

Applicant respectfully asserts that *Klein* is legally deficient for the purpose of anticipating claim 1. In particular, Applicant respectfully asserts that *Klein* does not teach or otherwise disclose at least the features/limitations emphasized above in claim 1. Therefore, Applicant respectfully requests that the rejection of claim 1 be removed.

Since claims 5 and 7 are dependent claims that incorporate all the features/limitations of claim 1, Applicant respectfully requests that the rejection of these claims also be removed. Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

With respect to claim 12, that claim has been amended to recite:

> 12. A system for enabling secure communication of information between a first network device and a second network device via the Internet, said system comprising:
>
> a secure tunnel system communicating with the Internet;
>
> the secure tunnel system being configured to:
>
> provide address information to a first network device via the Internet;
>
> receive encrypted information from the first network device via the Internet;
>
> ***post the encrypted information using a first one-time use URL associated with the address information; and***

> ***enable a second network device to access and retrieve the encrypted information via the Internet using a second one-time use URL while the encrypted information is posted.***

(Emphasis added).

Applicant respectfully asserts that *Klein* is legally deficient for the purpose of anticipating claim 12. In particular, Applicant respectfully asserts that *Klein* does not teach or otherwise disclose at least the features/limitations emphasized above in claim 12. Therefore, Applicant respectfully requests that the rejection of claim 12 be removed.

With respect to claim 19, that claim has been amended to recite:

> 19. A system for enabling secure communication of information between a first network device and a second network device, said system comprising:
>
> an information request system configured to communicate with the first and second network devices,
>
> the information request system being configured to receive an input from a user, the input corresponding to the user's intent to have encrypted information communicated to the second network device,
>
> the information request system being further configured to receive a decryption key and information corresponding to an address from the first network device in a secure format, the information request system providing the decryption key and the information corresponding to the address to the second network device in the secure format, thereby enabling the second network device to access and retrieve encrypted information posted on the Internet at the address and decrypt the information using the decryption key,
>
> ***wherein access to the address by the second network device is prevented after a predetermined period of time has elapsed, and***
>
> ***wherein the encrypted information is provided from the first network device to the second network device without either of the first and second network devices being identified to the other.***

(Emphasis added).

Applicant respectfully asserts that *Klein* is legally deficient for the purpose of anticipating claim 19. In particular, Applicant respectfully asserts that *Klein* does not teach or otherwise disclose at least the features/limitations emphasized above in claim 19. Therefore, Applicant respectfully requests that the rejection of claim 19 be removed.

Rejections Under 35 U.S.C. §103

The Office Action indicates that claims 2, 4, 13 – 15 and 17 - 18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Klein* as applied to claims 1, 12 and 19 and further in view of *Linden*. The Office Action also indicates that claims 6, 8 – 10, 16 and 20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Klein* as applied to claims 1, 12 and 19 and further in view of *Forslow*. The Office Action further indicates that claim 11 stands rejected under 35 U.S.C. 103(a) as being unpatentable over *Klein* as applied to claims 1 and further in view of *Rosenberg*, and that claim 3 stands rejected over the modified *Klein* and *Linden* method as applied to claim 2 and further in view of *Forslow*. With respect to claims 2, 4, 14, 15 and 17, Applicant has canceled these claims and respectfully asserts that the rejection as to these claims has been rendered moot. With respect to the remaining claims, Applicant respectfully traverses the rejection.

In this regard, the Office Action indicates that *Linden* teaches the use of one-time URLs. However, Applicant respectfully asserts that the pending claims patentably distinguish over Linden's use of one-time URLs. Specifically, *Linden* generally involves providing secure URL-based access to private resources.

In particular, *Linden* discloses:

> In a Web site system in which different private records or other resources are personal to different users, a method is provided for allowing users to securely access a private resource without the need to enter a username, password, or other authentication information, and without the need to download special authentication software or data to the user's computer. ***Each resource is assigned a private uniform resource locator (URL) which includes a fixed character string and a unique token***, and the URLs are conveyed by email (preferably using hyperlinks) to users that are entitled to access such resources. The tokens are generated using a method which distributes the tokens substantially randomly over the range of allowable token values ("token space"). The token space is selected to be sufficiently large relative to the expected number of valid tokens to inhibit the identification of valid tokens through trial and error. When a user attempts to access a private URL (such as to access a private account information page), a token validation program is used to determine whether the token is valid. ***The method may be used to***

> ***provide users secure to access private account information on the Web site of merchant. Other practical applications include electronic gift certificate and coupon redemption, gift registries, order confirmation electronic voting, and electronic greeting cards.***

(*Linden* Abstract). (Emphasis added).

Additionally, *Linden* discloses:

> Another practical application (not separately illustrated) involves sending the user 70 (FIG. 2) an email document 72 or ***a Web page which includes a one-time-use URL (preferably as a hyperlink 74) to a private discount page 78.*** The discount page 78 may, for example, give the user a 10% discount off the user's next purchase. Other users of the system would be sent like emails but which contain different tokens. In this application, the server application 40 would use the tokens to prevent users from obtaining multiple discounts. ***This may be accomplished, for example, by deleting each issued token from a table once the token has been used.***

(*Linden* at column 11, lines 17 - 28). (Emphasis added).

Based on the representative teachings of *Linden* above, several aspects of distinction between Linden and the pending claims are apparent. First, *Linden* does not involve the using two one-time URLs to transfer information from a first network device using a first of the URLs to a second network device using the second of the URLs. Second, *Linden* does not involve transferring information between first and second network devices without either of the first and second network devices being identified to the other. None of the other references teach or reasonably suggest these features either.

In this regard, Applicant has amended claim 1 to recite:

> 1. A method for securely communicating information, said method comprising:
>
> communicating an address to a first network device via the Internet such that the first network device provides information corresponding to the address for use by a second network device;
>
> receiving encrypted information from the first network device via the Internet;
>
> enabling the encrypted information to be posted at the address; and
>
> enabling the second network device to access the address and retrieve the encrypted information posted at the address;
>
> ***wherein the address provided to the first network device is a first Uniform Resource Locator (URL) configured for a one-time use; and***

> ***wherein the second network device retrieves the encrypted information using a second URL, the second URL being configured for a one-time use.***

(Emphasis added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 1 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 1. Therefore, Applicant respectfully asserts that claim 1 is in condition for allowance.

Since claims 3 and 5 – 11 are dependent claims that incorporate all the features/limitations of claim 1, Applicant respectfully asserts that these claims also are in condition for allowance. Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

With respect to claim 12, that claim has been amended to recite:

> 12. A system for enabling secure communication of information between a first network device and a second network device via the Internet, said system comprising:
>
> a secure tunnel system communicating with the Internet;
>
> the secure tunnel system being configured to:
>
> provide address information to a first network device via the Internet;
>
> receive encrypted information from the first network device via the Internet;
>
> ***post the encrypted information using a first one-time use URL associated with the address information; and***
>
> ***enable a second network device to access and retrieve the encrypted information via the Internet using a second one-time use URL while the encrypted information is posted.***

(Emphasis added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 12 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 12. Therefore, Applicant respectfully asserts that claim 12 is in condition for allowance.

Since claim 13 is a dependent claim that incorporates all the features/limitations of claim 12, Applicant respectfully asserts that this claim is also in condition for allowance. Additionally, this claim recites other features/limitations that can serve as an independent basis for patentability.

With respect to claim 16, that claim has been amended to recite:

> 16. A method for securely communicating information, said method comprising:
> providing a first network device;
> receiving, at the first network device, an address via the Internet;
> receiving an input from a user, the input corresponding to the user's intent to have information communicated to a second network device;
> in response to the user input, establishing communication with a third network device via the Internet, the third network device being configured to provide the first network device with a first Uniform Resource Locator (URL) for use by the first network device and a second URL for use by the second network device, ***the first URL being configured for a one-time use such that the first network device can post encrypted information at the address using the first URL, the second URL being configured for a one-time use such that the second network device can retrieve the encrypted information from the address using the first URL; and***
> ***receiving the first and second URL's from the third network device.***

(Emphasis added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 16 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 16. Therefore, Applicant respectfully asserts that claim 16 is in condition for allowance.

Since claim 18 is a dependent claim that incorporates all the features/limitations of claim 16, Applicant respectfully asserts that this claim is also in condition for allowance. Additionally, this claim recites other features/limitations that can serve as an independent basis for patentability.

With respect to claim 19, that claim has been amended to recite:

> 19. A system for enabling secure communication of information between a first network device and a second network device, said system comprising:
>
> an information request system configured to communicate with the first and second network devices,
>
> the information request system being configured to receive an input from a user, the input corresponding to the user's intent to have encrypted information communicated to the second network device,
>
> the information request system being further configured to receive a decryption key and information corresponding to an address from the first network device in a secure format, the information request system providing the decryption key and the information corresponding to the address to the second network device in the secure format, thereby enabling the second network device to access and retrieve encrypted information posted on the Internet at the address and decrypt the information using the decryption key,
>
> ***wherein access to the address by the second network device is prevented after a predetermined period of time has elapsed, and***
>
> ***wherein the encrypted information is provided from the first network device to the second network device without either of the first and second network devices being identified to the other.***

(Emphasis added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 19 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 19. Therefore, Applicant respectfully asserts that claim 19 is in condition for allowance.

Since claim 20 is a dependent claim that incorporates all the features/limitations of claim 19, Applicant respectfully asserts that this claim is also in condition for allowance. Additionally, this claim recites other features/limitations that can serve as an independent basis for patentability.

Newly Added Claims

In this response, Applicant has added new claims 21 - 25. Applicant respectfully asserts that these claims are in condition for allowance and that no new matter has been added. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claims 1, 12, 16 and 19, respectively, as lacking in the cited art. Since each of claims 21 – 25 is a dependent claim that incorporates all the features/limitations of either claim 1, 12, 16 or 19, Applicant respectfully asserts that these claims also are in condition for allowance. Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

Cited Art Made of Record

The cited art made of record has been considered, but is not believed to affect the patentability of the presently pending claims.

CONCLUSION

In light of the foregoing amendments and for at least the reasons set forth above, Applicant respectfully submits that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

Respectfully submitted,

David R. Risley, Reg. No. 39,345

THOMAS, KAYDEN,
HORSTEMEYER & RISLEY, L.L.P.
Suite 1750
100 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450,
on 7/25/05.

Stephanie Riley
Signature